COMPUTER SECURITY EDUCATION

Past, Present and Future

Carol Taylor, Rose Shumba, and James Walden

University of Idaho, Indiana University of Pennsylvania, and Northern Kentucky University

Abstract: This paper presents an overview of computer security education in academia. We examine security education from its recent past in the late '90's, evaluate its present state and discuss its future potential. A brief history of government programs that affect security education is presented along with their role as funding sources. The software industry perspective on security education and their relationship with academic security programs is also discussed. We define goals and objectives for the future of academic computer security programs and address barriers to successful achievement of those goals.

Keywords: Computer security education, computer science education, curriculum development, computer security

1. INTRODUCTION

Computer security became a tangible Computer Science sub discipline in the 1970's as the need to protect information became important with growing computer use in government and industry. At that time computer security research was funded by the military and primarily aimed at the protection of sensitive information. Computer security researchers and practitioners were few in number, worked primarily in the defense industry, and were mostly self taught.

Today, 30 years later, computer security is well established as an area of research and study within Computer Science. There are defined career paths for computer security professionals and an array of professional training and academic degree programs. If we compare the activity and interest in the field of computer security with its inception, one can say that a great deal of progress has been made. Yet, there is ample evidence that much more remains to be done.

Popular press reports describe daily the number of vulnerabilities found and the latest abuse of our systems by individuals in search of easy profit. Tumbleweed Communications, an e-mail security provider estimates that two-thirds of all e-mail is illegitimate traffic [1]. Botnets which consist of hacker-controlled networks of thousands of hosts are one of the fastest growing menaces on the Internet. These networks are capable of launching DDoS attacks, untraceable spam relays and widespread malware attacks [2]. SEI/CERT has stopped reporting incidents since they feel that widespread use of automated attack tools are so common that incident counts no longer provide meaningful information [3].

Several well-respected Computer Security researchers and educators also question the state of our knowledge and practice as a discipline. Roger Schell describes how the lack of science in computer security has actually led to a decline in the number of secure systems from a peak in the

1990’s [4]. Eugene Spafford, also questioned the quality of security practice in his paper, *A Failure to Learn From the Past* [5]. Spafford recounts the 1988 Internet worm incident and points out that the same conditions that allowed the worm to wreck havoc on systems still exist in 2003 nearly 15 years later.

As security researchers, it is discouraging to see the low level of practice in the *real world* with the constant stream of new system vulnerabilities and the increasing number of malicious programs in search of one of the many unpatched systems. But, as educators, we are hopeful that in time, through education, we can improve the current state of computer security by producing students trained in secure coding, with knowledge of secure system design and operation.

While there are multiple studies in the security education literature that document experiences of individual departments in developing academic security programs, there is at present no general study of security education[1]. Our motivation for this paper is our belief that a current overview of computer security education is needed in order to assess overall progress within the discipline and offer possible future directions.

In this paper, we examine the state of computer security education from the past, present and future. We include views from three separate groups that have a strong interest in security education: academia, government and industry. We review the state of academic security education since 1997, the year of the first CISSE conference [6], in order to assess progress over the past eight years. We then evaluate the current state of computer security education plus provide personal insights from our respective programs in computer security. In the last part of the paper we discuss the future of security education in terms of goals and objectives and note possible barriers to progress.

The paper is organized as follows: this section provides background and our motivation for the paper, Section two examines the progress made in computer security education in the past eight years, Section three presents the current state of security education and research funding, Section four describes our respective experiences in security curriculum development, Section five discusses the future of academic computer security programs and Section six concludes the paper by highlighting the future status of computer security education.

2. COMPUTER SECURITY EDUCATION IN THE PAST

In this section we trace the evolution of government initiatives for academic computer security education over the past eight years. We provide statistics on the programs and the events in government that have influenced the overall progress of the early academic security programs. We also briefly mention the state of early academic programs.

2.1 Academic Programs

Early academic programs in INFOSEC education were primarily for graduate students. Consequently, undergraduates wanting to learn about computer security had to take graduate courses or do so through independent study. Graduate level security courses typically concentrated on Multi-level Security [2](MLS) concepts or simply covered cryptography without a lot of practical system analysis [23].

[1] There are two CISSE keynote speeches by Matt Bishop in 1997 [23] and 2000 [24] that provide overviews of security education, but they are currently out of date.

[2] MLS handles the government's need for multiple classification levels for information such as unclassified, confidential, secret and top secret.

2.2 Government Support for Academic Programs

The first NCISSE conference was held in 1997 and was established as a forum for dialog between government, industry and academia to define requirements for information security education and encourage development and expansion of information security curriculum at the graduate and undergraduate levels [6]. This conference was the earliest official forum to recognize computer security and bring together academics teaching security with key people in industry and government (Figure 1).

Around the same time 1996-1999, President Clinton established the President's Council on Critical Infostructure Protection (PCCIP) and subsequent President Decision Directive 63 (PDD63) [7]. In establishing the PCCIP, the president recognized the vulnerability of the US infrastructure and acknowledged its importance to national security. PDD63 simply expanded the definition of critical infrastructure to include cyber security [7].

Soon after PDD63 appeared, in 1999, NSA established the Centers for Academic Excellence in Information Assurance (CAEIA) [8]. These centers were academic institutions with expertise in cyber security as demonstrated by a number of security oriented faculty and curriculum that met federal security training standards [8]. The purpose of this program was to increase the number of "security professionals of different disciplines". During the first year, seven schools[3] were established and recognized at the Third Annual NCISSE conference [7].

In February of 2000, President Clinton released the National Plan for Information System Protection [9] which established the Scholarship for Service (SFS) program managed by the National Science Foundation (NSF) [10]. This program provided scholarships for undergraduate and graduate students for up to two years in exchange for an equal amount of Federal Job service upon graduation. In order for a school to obtain a scholarship program, they must first qualify as a Center for Academic Excellence [8]. During the first two years of the program, 150 students were enrolled [11].

In 2002, President Bush created the Department of Homeland Security (DHS) which united 22 agencies into one common group for the purpose of improving homeland security. One of their responsibilities was and continues to be funding R & D for new scientific understanding and technologies in support of Homeland Security [12].

In 2003, the President's National Strategy to Secure Cyberspace was passed by President Bush. It identified four major actions and initiatives for awareness, education and training which include [13]:

1. Promote awareness nationally to empower all Americans to secure their own systems.

2. Foster training and education programs to support national and cyber security needs.

3. Promote private sector to support widely recognized cyber security certification and training programs.

4. Increase efficiency of existing federal cyber security training programs.

[3] These schools were: James Madison University, George Mason University, Idaho State University, Iowa State University, Purdue University, University of California at Davis, and University of Idaho.

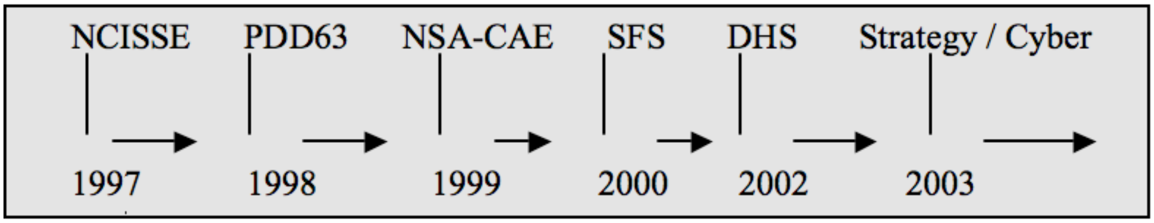

Figure 1. Timeline of Events Affecting Security Education

From 1997 to 2003, the US government created many initiatives for cyber security which appeared to recognize its importance for national security and the continued well-being of our nation. However, the only money allocated to academic security education was from the NSF SFS program.

3. COMPUTER SECURITY EDUCATION IN THE PRESENT

We now look at the present state of computer security education. We review the growing body of literature on established academic programs and discuss the typical approaches for establishing programs. Security education standards are discussed plus government and industry influences.

3.1 Academic Programs

Recently, a number of colleges have reported on their experiences adding computer security to their programs. Most schools appear to take one of two approaches: integrate security within individual CS courses [14, 15, 16] or create a special computer security degree or track[4] [17,18,19]. A few schools have opted for a combined approach where they have both specialized and integrated courses [20, 21]. There are reasons as to why a university chooses one approach over the other in their development of a computer security emphasis which often includes factors beyond the control of the institution. There are also tradeoffs with regards to these alternative approaches to computer security education.

Schools that choose to create a computer security track or special degree appear to have faculty that have experience in computer security or are strongly interested in pursuing security training [20, 19]. There also appears to be department or institutional support for a Security track and at least enough funding for course development. Integrating security into existing CS courses without offering specialized Security courses is one way that schools with limited resources in terms of faculty or funding can still offer security to students within their programs [14]. Faculty in these programs do not need not be retrained or develop completely new courses.

The effectiveness of each approach relates back to the goals for the CS graduates of a particular program in terms of computer security expertise. Programs that want to produce graduates with strong computer security skills capable of obtaining a computer security position have created specialized programs in computer security. CS programs that want their students to have exposure to computer security but not necessarily produce computer security professionals can achieve this through an integration of security principles into existing CS classes.

There is no clear evidence that specialized courses in computer security are superior to standard CS courses with integrated security components. However, schools that have chosen to integrate security within their existing curriculum point out several advantages over the specialized course path [14, 21]:

[4] Included are the schools that establish one or two specialized Computer Security courses

- Provide a security foundation to all their CS students as opposed to only those with a security interest

- Security concepts are learned within the broader CS topics such as system design, network administration, and programming

- The approach is available to all schools even those with limited resources and only requires faculty creativity and motivation

3.2 Government Support of Academic Programs

As discussed in Section 2.2, the government has several programs that currently support academic computer security education. Many of these programs were begun as the result of government initiatives related to national security. Here, we view the current status of these programs.

NSA-DHS Centers of Academic Excellence in Information Assurance [8]
Current: Has 67 Centers in 27 states
Started: 7 schools
Funding: Provides no monetary support for the Centers

NSF Scholarship for Service Program [10]
Current and Future: 350 graduates by 2005
Started: 150 enrolled
Funding: An annual budget of $30.5 million

The programs directly support Computer Security education within academic institutions. These programs appear to be thriving with an increasing number of Centers and students enrolled in scholarship programs.

3.2.1 Research Funding

In order to provide incentives for faculty and attract students into a field, the field of computer security needs a certain level of support in research dollars. Research fuels education by providing opportunities for faculty to publish, students to work on projects, and money to purchase equipment [23, 20]. Several long-time researchers and educators have noted that Computer Security needs a continued long-term commitment of basic research funding if it is to sustain itself as a viable area of study [22, 23].

At the first NCISSE conference in 1997, Bishop [23], a computer security researcher and educator, discussed the need for long-term funding as providing a stable base of resources and people which could be drawn from without having to continually start from scratch. In a later talk at CISSE[5] in 2000, Bishop commented that the government appears to be offering no support for basic security research which he states could ultimately prove disastrous [24].

Spafford briefed congressional staff in July, 2005 on the serious lack of funding in cyber-security research [22]. Spafford's group, the Presidential Information Technical Advisory Committee (PITAC)[6], issued a report in spring of 2005 that condemned the meager government investment in computer security research. Spafford noted that the NSF has become the primary agency for funding cyber security research with an annual budget of $30 million a year. This

[5] Between 1997 and 2000, NCISSE was changed to CISSE which is how it is currently known

[6] The group was disbanded in June of 2005

translates to only 8% of proposals being funded which as pointed out by the Computer Research Association (CRA) is discouraging student entry into the field [22].

The lack of long-term research funding was also noted by the Cyber Security Industry Alliance (CSIA), a group of security vendors who re-iterated PITAC findings in their own report [25]. The CSIA report stated that the Department of Homeland Security's budget in FY05 for science and technology is over $1 billion but that the budget for cyber security is just $18 million or about .02% [25].

Andy Birney, the editor of *Infosecurity* magazine, holds the government partly responsible for the nations' current cyber-security problems. Birney claims that a lack of government investment in security research discourages PhD students from entering the field [26]. This in turn creates shortages of faculty trained in security at academic institutions that produce the students entering the work force as programmers.

Another recent funding trend that affects computer security programs is the significant cuts from DARPA spending for university research [27]. DARPA has been a long-term source of basic Computer Science research funding for many years. This past year DARPA has cut the portion that goes to universities from $214 million to $123 million. They have shifted away from general research projects to more concrete deliverables produced in shorter time frames. This shift has resulted in a huge increase of proposals being directed towards NSF as one of the last Computer Science funding sources [27].

3.3 Industry View of Academic Programs

The computer industry comprises an important part of the United States economy, and almost all modern products and services use computer software. In the Report of the 2nd National Software Summit, leaders from academia, industry, and government argued that software should be elevated to an issue of national importance with a goal of "*Achieving the ability to routinely develop and deploy trustworthy software products and systems, while ensuring the continued competitiveness of the U.S. software industry"* [28]. The Build Security In (BSI) Software Assurance Initiative from the Department of Homeland Security seeks to achieve that goal in collaboration with academia and industry [29]. However, few companies accept responsibility for the poor quality of software that exists in most commercial products. Instead, some within the industry blame universities for producing programmers that don't know how to produce secure code.

Davidson, CSO of Oracle, appears to be a leading critic of academia [30, 31]. She believes academia should help shape the CS field and foster a culture of security. Davidson believes academia should produce CS majors that place more value on properties of safety, security and reliability above coolness and elegance. Davidson does not feel that industry should have to train programmers in security coding practices since they should have already acquired these skills prior to graduation [30].

Another group of software companies including Oracle and Microsoft, among others, discussed the failure of academic programs to produce security conscious programmers at a San Francisco Secure Software Forum in February, 2005 [31].

However, others point out that academia can't be entirely responsible for the problem of secure code. One panel member from the Secure Software Forum blames software companies that are still putting features above security [29]. The view that its partly industry's fault that we have so much bad software is supported by Birney as mentioned in Section 3.1. Birney refutes the popular belief that the root cause of vulnerabilities is insecure coding [26]. He discusses secure coding from three perspectives: academia, industry and government. Birney believes that a lack of government funding for academic computer security programs leads to a shortage of faculty with backgrounds in security as was discussed in the previous section. Furthermore Birney shifts some of the responsibility for vulnerable software to industry that still places development speed and profit over security.

While many in industry seem eager to blame academia for bad software without doing anything to help the situation, Microsoft is an exception in that they are working to fix the perceived problem. In 2002, Microsoft shut down for several weeks in order to train its workforce in secure software development [32]. Furthermore, they are one of the few companies investing in academic education through their 2-year old *Trustworthy Computing* curriculum program. They are offering $750,000 in grant money to 15 universities to produce security related curriculum. The curriculum materials are then made publicly available on their web site.

4. INSTITUTIONAL EXPERIENCES IN SECURITY PROGRAM DEVELOPMENT

In this section we offer the authors' individual experiences in Computer Security program development. Each program is different and is representative of various types of schools that develop security expertise in CS. The University of Idaho represents a mature, long-term security program since they were one of the original designated NSA CAE's. Indiana University of Pennsylvania is a more recently designated CAE (2002) and represents a less established security program. The computer security program at Northern Kentucky University is the smallest of the three and represents a non-CAE program that is mostly based on the efforts of a single faculty.

In establishing security programs at all three schools there were several commonalities noted. All three schools noted some difficulty with a lack of computer security curriculum standards. All programs began as the effort of one (or a few) faculty who instigated the security effort. All three schools are not major universities with large amounts of funding, so these programs were established in spite of limited funding. Students at the schools appear to be very interested in the topic and enrollment in the programs continues to be strong.

4.1 University of Idaho

Information assurance curriculum development at the University of Idaho began in 1991 with the arrival of Dr. Jim Alves-Foss. Dr. Alves-Foss graduated from UC Davis with a specialty in computer security and became the first IA faculty at the University of Idaho. The first security course developed consisted of a combined upper division undergraduate and graduate course, in computer security that emphasized both theory and practical knowledge. The addition of a second IA faculty, Dr. Debra Frincke, in 1993 resulted in the creation of several more security courses, Network Security and a senior/graduate level seminar in Intrusion Detection.

These early courses were followed by a senior/graduate course in Survivable System Analysis, a seminar in Security Policies and a course in Exploit Techniques and Defense. Other CS faculty became interested in IA and assisted with the development and teaching of these courses. In 2004, several additional courses were added including Forensics analysis and a lower level general Security Course [33]. These courses evolved as the perceived need arose and as an outgrowth of faculty research interests.

During the period of our curriculum development effort, we became an NSA CAE/IAE [8] and also participated in the NSF Scholarship for Service (SFS) program [10]. The NSA program has certain curriculum requirements which must be met in order to qualify for program continuance. The NSA CAE/IAE designation is closely tied to the National Security Telecommunications and Information Systems Security Committee's, NSTISSI[7] training standards especially 4011. In becoming an Academic Center of Excellence, the institution must

[7] In 2001, by Executive Order , NSTISSC was re-designated as CNSS, the Committee on National Security Systems.

demonstrate that their curriculum complies with the 4011 standard plus at least one other standard selected from the 4012 – 4015 documents [34]. Certification verifies that the college teaches skills that cover each of the seven topic areas of 4011.

In 2005, we have also begun integration of security concepts within several of our standard CS courses. We are planning on introducing secure coding into our beginner coding classes plus a computer security integrated software engineering class.

4.2 Indiana University of Pennsylvania

Indiana University of Pennsylvania (IUP) was designated a Centre of Academic Excellence in 2002. Since then, there has been noticeable improvement in curriculum development:

In 2003, a Bachelor of Information Assurance degree, jointly offered by the Computer Science department and the Criminology department track was introduced.

In 2005, a Master of Science in Information Assurance was recently developed. This is an interdisciplinary program designed to meet the industry and government needs for computer/network/information security professionals. The first offering will be in the fall of 2006.

- Through the NSF Cyber Security Capacity Building grant of 2001 – 2002, NSA Capacity grant of 2002- 2003, and the 2003 Cisco Equipment grant of $88,000, IUP established two isolated security laboratories, the Cyber Security and the Information Assurance laboratories, for teaching and research purposes.

- Through the SIGSCE Special Projects fund and local IUP Senate funding, hands-on exercises for Information Assurance courses have been developed. These are being pilot-tested in the department.

- To gain an industrial perspective of information assurance, industry partners provide guest lecturers on legal issues in Information Assurance classes and at the Information Assurance club meeting plus state police consultants provide guest lectures on legal issues.

One challenge in computer security education is the lack of body of knowledge for the computer security curriculum. During the summer of 2003 we started a project on augmenting and improving the teaching of the Cybersecurity Basics course at IUP. The Cybersecurity Basics course is an interdisciplinary course for the Criminology, Management Information Systems and Computer Science students. The course provides an introduction to the theories and concepts of computer security in host systems. The project involved 1) evaluating the effectiveness of host security tools in defending systems. 2) developing hands-on lab exercises based on the evaluated tools, and 3) integrating the developed hands-on lab exercises and the Cybersecurity theories and principles. Nine lab exercises were developed.

The development of teaching materials for Information Assurance courses can be a challenge. Most of the hands-on exercises required for such courses are based on tools for intrusion detection, forensic analysis, vulnerability analysis, firewall setting up, router auditing and packet sniffing. The challenge is that there is an abundance of CERT recommended security tools, tool version are changing often, and the teaching materials need to be continually updated.

4.3 Northern Kentucky University

Computer security curriculum development began at Northern Kentucky University (NKU) in 2002 with the introduction of a graduate computer security course by Dr. Charles Frank. Undergraduates enrolled in the class as a senior-level special topics elective course. The course focused on security fundamentals and network security and included a variety of lab exercises. The math department also offered a cryptology class, in which many computer science students enrolled.

In 2004, NKU added a new Computer Information Technology (CIT) degree with a track in Network, System Administration and Security. An undergraduate class in computer security was added as a requirement for the new track and as an elective for both CIT and CS majors.

NKU created a new College of Informatics in 2005, enhancing the ability of the departments of Computer Science and Information Systems to collaborate and hastening the pace of security curriculum development. Faculty designed a shared core curriculum for computer science, computer information technology, and information systems, and began mapping NKU's computer security curriculum to the CNSS 4011 standard as a preliminary step to becoming an NSA Center for Academic Excellence. The two departments will collaborate to offer a graduate certificate in Corporate Information Security in 2006.

The addition of a second faculty member, Dr. James Walden, with prior experience teaching computer security at the University of Toledo, helped the Department of Computer Science design new classes in Computer Forensics, Network Security, and Secure Software Engineering. The department is also beginning to integrate secure coding techniques into classes with a focus on programming. Building on the department's strengths in software development, a graduate certificate in Secure Software Engineering will be offered starting in 2006. Future plans include construction of a dedicated network security lab and development of a Master of Science degree program in Secure Software Engineering.

5. COMPUTER SECURITY EDUCATION IN THE FUTURE

So far, we have addressed the recent past of computer security education, *where we have been*, and the present, *where we are* with regards to programs, government and industry involvement. In this section, we discuss the future, *where we are going* with particular attention to objectives and potential barriers to success.

5.1 Computer Security Education Objectives

In trying to visualize the future of computer security education, it is useful to set goals and define specific objectives for reaching those goals. No one in the security field would argue with the general belief that providing a security background is beneficial to all students graduating from CS departments. One overall goal would be to increase the number of CS graduates with an understanding of computer security principles. Consequently, one objective that would help in reaching this goal is to increase the number of CS programs that teach computer security. Analyzing the specific steps needed to realize the objective of expanding the security education programs leads to a discussion of barriers to success for computer security education, the topic of the next section.

5.2 Barriers to Success for Computer Security

Achieving the objectives of promoting or increasing security concepts in CS programs requires some investment on the part of both institutions and the faculty member(s). These respective responsibilities for faculty and institutions are outlines in Table 1.

Table 1. Responsibilities for Promoting Computer Security

Responsibilities	
Institution	Faculty
Reduced Teaching Load	Learn Computer Security
Travel and/or Training Support Grants	Collaborate with Computer Sec. Research Inst.
Tenure Support	Travel to Conferences

In addition to the specific activities of faculty and institutions that wish to add computer security to the curriculum, there are other possible barriers to establishing a computer security emphasis. These are outside the control of faculty and their colleges and include:

- No standard for CS curriculum development
- Lack of government funding in basic research
- Limited industry involvement

Each of the barriers is explained in terms of its relations to computer security education.

There is currently no accepted standard for college level computer security curriculum development. This presents a barrier to the development of computer security programs. Without an accepted standard, departments must work harder to define course content [14, 19]. The lack of an academic computer security curriculum standard was recently studied by one of the authors [35]. That study noted the inadequacy of the 40XX Training Standards for academic programs and described the problems faced by academia in trying to map their curriculum to these standards.

The lack of government funding was addressed in a previous section and noted as a disincentive for promotion of security education. If there is little or no research funding available in a given field of study, then there is no way to support graduate students who are to become future faculty and eventually promote their own research programs. Consequently, disciplines that lack research support struggle to recruit students and faculty since there is a perception of a lack of resources in the field. The current dismal situation where only a small percentage of cyber security proposals are funded by the NSF is not conducive to promoting computer security programs within academia.

The software industry is concerned with the perceived lack of security awareness in students graduating from CS programs. Yet, they are not as a group volunteering to assist with this problem either by funding or other direct involvement. The objectives of the CISSE conference were to establish a working partnership between government, industry and academia [6]. Industry and government should provide better support for higher education. Yet, outside of the institutions with large, well-established programs, partnerships between industry and academia are not common. In addition to directly funding academic research projects, industry could provide a number of other opportunities. There could be an exchange of faculty and industry in internship settings in order to share expertise, students could benefit by working on real problems [23], industry could serve on Department advisory boards.

6. CONCLUSION AND FUTURE WORK

In this paper, we have provided an overview of computer security education. We presented government initiatives and other events from the past eight years, examined the current state of academic progress and discussed future objectives for promoting security within CS along with the perceived barriers to success. There are a number of areas that need to be addressed in order for security education to progress. A lack of research funding in academic programs appears to be a major roadblock to the creation of a viable national security program. Faculty training along with institutional support appears to be a problem for programs that lack any faculty with a background in security.

6.1 Future Work

There is a strong need for a survey of CS and IT departments to determine current status, future plans and needs for security education. The University of Idaho is planning to survey schools that have mapped their curriculum to the CNSS[8] 40XX training standards to get feedback on their experience mapping their curriculum to the 40XX criteria. However this is intended to be a targeted survey and not a comprehensive survey of all CS departments.

Other projects that would benefit security education include:

– An academic curriculum standard for both undergraduate and graduate programs

– Integration of computer security into accreditation programs (e.g. ABET)

– Support for schools beginning security programs

  – Curriculum help and mentorship from established programs

Those who work in both security and education see promotion of security education for all graduating CS majors as one of the few concrete steps we can take that could favorably improve the state of cyber security. Ultimately, security education should increase the level of competence in our developers to produce better quality, more robust systems capable of surviving most disruptions, intentional or otherwise.

REFERENCES

1. Saita, A. “Ripe for Harvest”, Information Security, Vol. 8.3, March 2005.
2. Dittrich, D. “Invasion Force”, Information Security, Vol. 8.3, March 2005.
3. Landwehr, C. E., “Changing the Puzzle Pieces”, IEEE Security & Privacy, Vol. 3,1, Jan/Feb 2005
4. Schell, R. "Information Security: Science, Pseudoscience and Flying Pigs", Invited Essay, ACSAC 2001.
5. Spafford, E. "A Failure to Learn from the Past", ACSAC, 2003, http://www.acsac.org/2003/papers/classic-spafford2.pdf
6. CISSE. “Colloquium for Information Systems Security Education”, http://www.nisse.org
7. PCCIP and PDD63. http://www.ciao.gov/PCCIP/report_index.html
8. NSA. “NSA Centers for Academic Excellence", http://www.nsa.gov/isso/programs/nietp/newspg1.htm
9. National Plan for Information System Protection. http://www.gao.gov/new.items/d02474.pdf
10. National Science Foundation Scholarship for Service. http://www.sfs.opm.gov
11. NSF SFS Statistics, http://www.internetnews.colm/bus-news/article.php/1585651
12. Department of Homeland Security. Announcement. http://www.dhs.gov/dhspublic/display?theme=10
13. Null, L. "Integrating Security Across the Computer Science Curriculum", Consortium for Computing Sciences in Colleges, (CCSC) 2004.
14. Irvine, C.E., Chin, S. and Frincke, D., "Integrating Security into the Curriculum", IEEE Computer, pp. 25-30, December 1998
15. Mullins, P. et. al. "Panel on Integrating Security Concepts into Existing Computer Courses", SIGCSE '02, Feb. 27 Mar. 3, 2002, Covington, KY, 2002.

[8] In 2001, the President re-designated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS) which resulted in a renaming of the training standards to CNSS instead of NSTISSC

16. Werner, L. "Teaching Principled and Practical Information Security", Consortium for Computing Sciences in Colleges, (CCSC) 2004.
17. Azadegans, S. et. al. "An Undergraduate Track in Computer Security", ACM SigCSE Bulletin, Vol. 35, 3, June 2003.
18. Crowley, E. "Information System Security Curricula Development", Proceed. of Conf. on Inform. Tech. Curriculum (CITCA '04), Oct. 16-18, 2003, Lafayette, IN.
19. Vaughn, R. Jr., Dampier, D. and Warkentin, M. B. "Building an Information Security Education Program", InfoSecCD Conference '04, Oct. 8, 2004, Kennesaw, GA
20. Yang, A. "Computer Security and Impact on Computer Science Education", Jr. of Computing in Small Colleges, Vol. 16, 4, April, 2001.
21. Computer Research Association Policy Blog. http://www.cra.org/govaffairs/blog/index.php
22. Bishop, M. The State of INFOSEC Education in Academia: Present and Future Directions, keynote speech, NCISSE, pp 19-33, Apr. 1997.
23. Bishop, M. "Computer Security Education: Training, Scholarship and Research", keynote speech, CISSE, 2000.
24. CSIA. "Federal Funding for Cyber Security R & D", CSIA Alliance, July 2005, http://www.csialliance.org/CSIA_RD.pdf
25. Birney, A. "Secure Coding? BAH!", Editorial, InfoSecurity, Jan. 2004.
26. Markoff, J. "Failure of Federal Cyber Security Funding", New York Times, June 2005.
27. CNSS, Report of the 2nd National Software Summit, http://www.cnsoftware.org/nss2report/NSS2FinalReport04-29-05PDF.pdf, April 29, 2005
28. Gary McGraw and Nancy Mead, "Engineering Security Into the Software Development Life Cycle ," Crosstalk: The Journal of Defense Software Engineering, October 2005, http://www.stsc.hill.af.mil/crosstalk/2005/10/0510McGrawMead.html
29. Davidson, M.A. "Leading by Example: the case for IT Security in Academia", Educause Review, Jan/Feb. 2005.
30. Lemos, R. "Software Firms Fault Colleges' Security Education", c/net News.com, Feb. 2005, http://news.com.com/Software+firms+fault+colleges+security+education/2100-1002_3-5579014.html
31. Microsoft Research. "Microsoft Curriculum Grants", http://www.microsoft.com/presspass/press/2005/jul05/07-18FacultySummit/05PR.mspx
32. CSDS. "CS Based IA Curriculum", http://www.csds.uidaho.edu/IA/IAStudy.htm.
33. NSA. "National IA Education and Training Program", http://www.nsa.gov/ia/academia/cnstesstandards.cfm
34. Taylor, C. and Alves-Foss, J. "The Need for Information Assurance Curriculum Standards", Proceedings of 2005 CISSE, June 6-9, Atlanta, GA, 2005.